

**SYSTEM AND ARRANGEMENT FOR PROCESSING PAYMENTS FOR
PURCHASES THROUGH A PAYMENT SERVER**

Inventors:

Jean-Marc Villaret
75/77 rue des Grands Champs
Paris, France 75020

William Stuart Taylor
10413 B Merriman Road
Cupertino, CA 95014

Kevin Frank Ritschel
579 Giant Way
San Jose, CA 95127

Assignee:

HEWLETT PACKARD COMPANY

SYSTEM AND ARRANGEMENT FOR PROCESSING PAYMENTS FOR PURCHASES THROUGH A PAYMENT SERVER

FIELD OF THE INVENTION

The present invention generally relates to Electronic Funds Transaction Point of Sale (EFTPOS) systems, and more particularly to processing payments for purchases
5 through non-conventional terminals and communication devices.

BACKGROUND OF THE INVENTION

Electronic Funds Transaction Point of Sale (EFTPOS) terminals and systems have operated for many years. Most current EFTPOS terminals function in the same manner in
10 that account data are input to the terminal, usually via a magnetic stripe reading device. A display and keypad are usually integrated with the EFTPOS terminal. The consumer is prompted to enter a personal identification number (PIN) associated with a debit card before the account data are sent to a bank or financial institution for payment authorization. Once authorization is received the transaction continues until completion,
15 for example, by receipt of article purchased and the sales receipt.

EFTPOS systems are highly secure systems that are designed to run a limited number of applications using a dial out modem. The modem is linked to servers that are controlled by financial institutions. Only authorized bank personnel are authorized to install or upgrade software applications residing in the EFTPOS terminals. PIN numbers
20 are not stored in the terminals, and tampering with any EFTPOS terminal is automatically detected and payment transactions through the tampered line are immediately suspended.

EFTPOS terminals are usually located adjacent the cash register in merchant locations for conveniently processing payments. Once the data are input to the terminal, the data are sent via a transaction-switching network to the host computer of the
25 customer's bank to obtain bank authorization. The merchant's bank coordinates the settlement of funds from the customer's bank to the merchant's bank.

Consumers that shop frequently on-line or pay their bills on-line try to balance convenience with risk since these transactions have relatively poor security safeguards. Despite the efforts of on-line vendors to improve the security of purchase transactions, the
30 fact that the transactions are being conducted over a public network, such as the Internet, makes it extremely difficult to prevent others from capturing sensitive information as it is

being transmitted over the public network. EFTPOS systems, on the other hand, provide a high level of security in processing payments due to controlled communications lines and complex protocols required by financial institutions. However, these transactions are limited to authorization of payments and electronic funds transfers that are not conducted over the Internet or any other public network. Any attempts to make EFTPOS systems more flexible have been deterred due to the number of different protocols that exist (since each financial institution has its own protocol and guidelines) and the requirement of controlling communications to maintain high levels of security. Personal computers do offer the convenience of entering your credit card number for on-line purchases.

However, payment security is compromised as a consequence of such convenience.

Further complicating efforts at improving payment processing security over unsecured communications networks is the advent of new marketing channels offering consumers more purchasing opportunities. For instance, products that are offered for sale via a mobile telephone or a PDA (personal digital assistant) require the consumer to call in to the vendor to effect payment. In another example, sales volume of selling products through cable TV shopping programs could be significantly increased if the payment processing for such purchases is streamlined from the current call-in system. Despite the opportunities that vendors have to access consumers in new ways, vendors and consumers must still transact payments through traditional POS terminals or by communicating credit card information through a traditional call-in system.

A method and a system that address the aforementioned problems, as well as other related problems, are therefore desirable.

SUMMARY OF THE INVENTION

The present invention is directed to addressing the above and other needs in connection with offering consumers an alternative for effecting payment for purchases over unsecured communication networks. In one example embodiment, a payment server arrangement facilitates receipt and processing of payment requests from various data communication devices, including POS terminals, without compromising the security of the transaction. Throughout this specification and in the claims, the term "product(s)" is used in reference to both products and services. In addition, the term "merchant" is used in this specification as the party that subscribes for the payment processing service and

receives payments. The present invention is exemplified in a number of implementations and applications, some of which are summarized below.

According to one aspect of the invention, a payment processing system includes a plurality of data communications devices that transmit a plurality of payment requests in connection with purchases via respective communication channels. Each transmitted payment request includes a merchant identification code and a set of customer financial account data. The system further includes a payment server arrangement that receives the payment requests from the data communications devices at the respective channels via a plurality of adapter modules corresponding to each of the communication channels. Each of the adapter modules includes a payment processing application that identifies a financial institution identification code associated with the merchant identification code. The adapter modules interface with a data processing system of the financial institution consistent with a communications protocol associated with the identified financial institution.

According to another aspect of the invention, a payment request processing arrangement communicates with a plurality of data communication devices via respective communications channels and with a plurality of data processing systems located at a plurality of financial institutions. The arrangement includes a payment server that is responsive to the plurality of data communications devices and is configured to receive a payment processing request via a first channel at a first adapter module corresponding to a first data communications device. Each payment request includes a merchant identification code and a set of customer financial account data. The first adapter module has a first payment processing application that identifies a financial institution identification code associated with the merchant identification code and interfaces with a data processing system of the financial institution consistent with a communications protocol associated with the identified financial institution.

According to yet another aspect of the invention, a computer-implemented method and system facilitates processing payment requests from a plurality of secured and unsecured data communications devices, wherein each payment request includes a merchant identification code and a set of customer financial data. The method includes providing a plurality of adapter modules, each adapter module configured to interface with one or more of the communications devices via a selected communications channel. The adapter modules receive payment requests from the data communications devices via the

communications channels. The financial institutions associated with the merchant identification codes are identified, with each financial institution having an associated data processing system for processing payment requests. The method also includes interfacing with the data processing systems of the financial institutions consistent with payment protocols associated with the financial institutions.

It will be appreciated that various other embodiments are set forth in the Detailed Description and Claims that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

Various aspects and advantages of the invention will become apparent upon review of the following detailed description and upon reference to the drawings in which:

FIG. 1 is a diagram of a payment request processing system that incorporates a payment server arrangement in accordance with an example embodiment of the invention; and

FIG. 2 is a flowchart illustrating the manner of processing payment requests from various secured and unsecured data communication devices in accordance with another example embodiment of the invention.

While the invention is amenable to various modifications and alternative forms, specifics thereof have been shown by way of example in the drawings and will be described in detail. It should be understood, however, that the intention is not to limit the invention to the particular embodiments described. On the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

DETAILED DESCRIPTION

Various embodiments of the present invention are described in connection with providing payment-processing services to merchants for facilitating payments made by customers not using traditional POS terminals. In addition, an enhanced payment processing system of the present invention will facilitate the addition of new data communications devices that communicate via distinct protocols and communication channels without the need to reconfigure the entire payment processing system. For purposes of this application, data processing systems (DPS) include, but are not necessarily limited to, personal computers, internet appliances, e-Service related entities

and objects, servers and workstations. Data communication devices include, but are not necessarily limited to, PDAs, mobile and WAP-enabled telephones and two-way pagers. Those skilled in the art will appreciate that the invention could be implemented in a variety of programming languages and hardware platforms.

5 In an example embodiment, a payment server serves as the front end of an electronic funds transfer point of sale (EFTPOS) system to process payments received from secured and unsecured data communication devices. For instance, a merchant subscribing to payment services provided by a CSP (Commerce Service Provider) can now offer his customers the convenience of paying for purchases via a mobile telephone
10 (or a set top box) with the security of a POS terminal. A payment server managed by the CSP processes payment requests received via various channels each with a distinct protocol. In one example, a payment request received at the payment server from a customer's set top box is in a protocol selected by the cable service provider and is processed by an adapter module configured specifically for the selected protocol. In
15 another example, payment requests received from SSL/SET enabled data communications devices are processed by another adapter module configured specifically for SSL/SET-based requests. The payment requests include a merchant identification code, a set of customer financial account data (e.g., credit card) and the purchase amount. In a related embodiment, the payment requests include a date and time and a purchase code. The
20 payment server receives the payment request at one of a number of adapter modules that are each configured to respond to each protocol of each communications channel. Each of the adapter modules includes a payment processing application that identifies a financial institution identification code associated with the merchant identification code. The adapter modules interface with a data processing system of the financial institution (or
25 bank) consistent with a communications protocol associated with the identified financial institution. Once the payment request is routed to the appropriate bank, then the request is handled as a normal ACH (automatic clearinghouse) transaction, which includes transferring funds from the credit card issuer to the merchant's bank.

Referring now to the figures, FIG. 1 illustrates a payment request processing
30 clearinghouse system 100 that incorporates a payment server arrangement 110 in accordance with an example embodiment of the invention. In this example, system 100 includes a payment processing system 102 that is communicatively coupled to data processing systems of a financial clearinghouse network 140. In particular, system 102

includes payment server arrangement 110 that receives payment requests from a plurality of data communications 120 via various communications links 130 having respective communications protocols. Payment server arrangement 110 includes a plurality of adapter modules 112-116, a merchant/bank identification code database 118 and a communications interface 113. Each of the adapter modules includes a payment processing application configured to process payment requests received in a distinctive protocol.

Payment server 110 also includes a processor arrangement (not shown) that processes incoming signals as well as a memory arrangement (not shown) that stores the payment applications. Once the payment request is processed through the adapter modules the payment request is forwarded through interface 113 to banks 142. Banks 142 perform the traditional clearinghouse tasks through merchant bank DPS 144 and through customer bank DPS 146. In related embodiment, a merchant transactions database 119 is configured to receive and store historical (processed) payment data for later use in demographic research.

In this example embodiment, POS adapter module 112 of payment server 110 includes a payment processing application 112A that is configured to receive payment requests from customers at POS terminals 122 via communications link 132. POS terminals 122A-122C read a credit card (or a smart card or a chip card) tendered by the customer to effect a purchase payment and transmit a set of the customer-specific financial account data to adapter module 112. In one embodiment, POS terminal 122A is a thin client POS that does not include memory or a microprocessor. Terminal 122A relays the payment request data immediately to adapter module 112 of server 110 for processing the payment request. Adapter module 112 of server 110 takes control of the interactions between terminal 122A and server 110 by sending commands to terminal 122A to display data, to send data to a PIN PAD display (not shown), send data to a printer or send data to the chipcard. Data includes payment amount, retail location, merchant identification codes, personal identification numbers or other information that needs to be relayed to financial network 140. Adapter 112 communicates with terminal 122A until the payment request is complete before forwarding the request to financial network 140 for processing.

In another example embodiment, terminal 122B is a "FAT" client POS that includes processing and memory capabilities as well as an integrated modem and software. Terminal 122B incorporates multiple applications and shares processing duties with server

110. Thus, the payment processing request is completed at terminal 122B before the request is encrypted and forwarded to adapter module 112 for further processing. A communications link 132 between terminals 122 and server 110 could be wireless (wireless WAN or cellular) or a standard communications network (e.g., modem to PSTN or LAN).

In this example embodiment, server 110 also includes adapter module 114 and an adapter module 116 that are configured to communicate with a set top box and SSL/SET-enabled communications devices, respectively. Adapter module 114 receives a payment request from a customer's set top box 124 via cable or satellite link 134. Payment processing application 114A of adapter module 114 identifies the financial institution 142 associated with the merchant identification code using database 118. In this example, database 118 also includes a description of the communications protocol used by the financial institution for network communications. Application 114A converts the payment request to an electronic format that is suitable for processing by the data processing system of the identified financial institution.

Similar to adapter module 114, adapter module 116 receives a payment request from a customer's mobile telephone or PDA 126 (SSL/SET-enabled communications device) via a wireless communications link 136. In a related embodiment, adapter module 116 receives the payment request only after the customer enables a customer-controlled server (not shown) to send the customer financial account data. The customer-controlled server includes financial account data of the customer that is only made available to third parties upon the customer's request. Transactions processed through the customer-controlled financial server are configured to be more secure than sending the credit card information directly for payment processing. Merchants are encouraged to use more secure alternatives for receiving payments from customers by paying processing fees that are related to the level of security of the payment processing channel. The more secure the processing channel the lower the fee that the merchant is charged per transaction. In one example, the merchant is charged a 2% fee of the value of the customer purchase when the customer uses the POS terminal 122 versus 6% when the customer sends the credit card information over an unsecured data communications line. Since the customer-controlled financial server is considered highly secure, transactions processed therethrough will be at a lower cost to the merchant.

One of the advantages to server 110 is the ability to retrofit older EFTPOS systems with server 110 to automatically upgrade the entire payment processing system. Server 110 provides older systems with the capability of processing payments from different sources without compromising security. New applications are easily added to server 110 without having to make hardware adjustments/changes at any of the data communications devices 120.

Other data communications devices for effecting payments include vending machines or kiosks that are configurable to communicate as POS terminals or as SSL/SET-enabled devices. Once configured, the vending machine and the kiosk appear to server 110 as remote data communications devices and the server processes the payment requests as usual.

In another example embodiment, another entry point (not shown) to payment server 110 includes data communication devices used by small merchants that do not have a fixed POS terminal location but have their own authorization line with a financial institution. In this example, a small merchant or a taxi driver uses a thin POS device (*e.g.*, mobile telephone) to enter the credit card number of the customer or passenger. In another example, the mobile telephone is WAP-enabled or utilizes the SMS (short message service) where he is operating in a GSM environment. The merchant then proceeds to send the financial account information along with his merchant identification code to server 110 for payment processing as described in the other related embodiments above.

In yet another example embodiment, another entry point (not shown) to payment server 110 for the customer includes, but is not necessarily limited to, a personal communications device (*e.g.*, PDA) and a smart card enabled mobile telephone. With these data communications devices, the customer sends the financial account data (*e.g.*, credit card number) with the merchant identification to server 110 for payment processing as described in connection with other related embodiments.

Referring now to FIG. 2, a flowchart 200 illustrates a computer-implemented method of processing payment requests from various secured and unsecured data communication devices in accordance with example embodiment of the invention. The payment requests include a merchant identification code and a set of customer financial data. In a related embodiment, time and date as well as a purchase code is included in the payment request. At step 202, the method includes providing a plurality of adapter modules 112-116 each of which is configured to interface with one or more of

10013448-1

communications devices 120 via a selected communications channel (e.g., 132). At step 204, adapter modules 112-116 receive payment requests from data communications devices 120 via the communications channels 130. At step 206, the financial institutions 140 associated with the merchant identification codes are identified, with each financial institution having an associated data processing system for processing payment requests. At step 208, the method also includes interfacing with the data processing systems of the financial institutions 140 consistent with payment protocols associated with the financial institutions. At step 210, payment processing occurs at the identified financial institution. At step 212, adapter module transmits a payment request status via the selected communications channel to one of the data communications devices 130.

Various embodiments of the invention are believed to be applicable to a variety of payment request processing systems. The present invention has been found to be particularly applicable and beneficial in scenarios involving payment processing requests using personal communications devices owned by the customer. Other aspects and embodiments of the present invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and illustrated embodiments be considered as examples only, with a true scope and spirit of the invention being indicated by the following claims.